HASSE INVARIANTS AND MOD p SOLUTIONS OF A-HYPERGEOMETRIC SYSTEMS

ALAN ADOLPHSON AND STEVEN SPERBER

Abstract. Igusa noted that the Hasse invariant of the Legendre family of elliptic curves over a finite field of odd characteristic is a solution mod p of a Gaussian hypergeometric equation. We show that any family of exponential sums over a finite field has a Hasse invariant which is a sum of products of mod p solutions of A-hypergeometric systems.

1. Introduction

Igusa[12] noted that when p is an odd prime, the Hasse invariant

$$H(\lambda) = (-1)^{(p-1)/2} \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 \lambda^i$$

of the Legendre family of elliptic curves $y^2 = x(x-1)(x-\lambda)$ over a finite field of characteristic p is a mod p solution of the Gaussian hypergeometric equation

$$\lambda(1-\lambda)y'' + (1-2\lambda)y' - (1/4)y = 0.$$

In fact, $(-1)^{(p-1)/2}H(\lambda)$ is congruent mod p to the truncation of the Gaussian hypergeometric series ${}_2F_1(1/2,1/2,1;\lambda)$ at $\lambda^{(p-1)/2}$. The numerator of the zeta function of the elliptic curve has a unit root if and only if $H(\lambda) \neq 0$. More precisely, let

$$Z_\lambda(T) = \frac{(1-\alpha_1(\lambda)T)(1-\alpha_2(\lambda)T)}{(1-T)(1-qT)}$$

be the zeta function of the (projectivized) elliptic curve over $\mathbb{F}_q$, $q = p^a$, when $\lambda \neq 0, 1, \infty$, where $\alpha_1(\lambda)$ denotes the unit root when λ is not supersingular. Dwork[10, Equation (6.29)] gave a formula for $\alpha_1(\lambda)$ in terms of values of (analytic continuations of) p-adic hypergeometric functions. The reduction mod p of Dwork's formula is

$$\alpha_1(\lambda) \equiv H(\lambda)H(\lambda^p)\cdots H(\lambda^{p^{a-1}}) \pmod{p}.$$

The purpose of this article is to give a generalization of this congruence to arbitrary families of exponential sums. In the process we extend earlier work of Beukers[6] describing mod p solutions of A-hypergeometric systems.

Let p be a prime, let $\mathbb{F}_q$ be the finite field of $q = p^a$ elements, and let

$$f_\lambda = \sum_{j=1}^N \lambda_j x^{\mathbf{a}_j} \in \mathbb{F}_q[x_1^{\pm 1}, \dots, x_n^{\pm 1}].$$

Date: September 13, 2012.

Put $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_N\} \subseteq \mathbb{Z}^n$. We make no assumptions on A until Section 7. Let $\Psi : \mathbb{F}_q \to \mathbb{Q}_p(\zeta_p)^\times$ be a nontrivial additive character and let $\omega : \mathbb{F}_q^\times \to \mathbb{Q}_p(\zeta_{q-1})^\times$ be the Teichmüller character. We consider the exponential sum

$$S(f_\lambda, \mathbf{e}) = \sum_{x=(x_1,\ldots,x_n)\in(\mathbb{F}_q^\times)^n} \omega(x_1)^{-e_1} \cdots \omega(x_n)^{-e_n} \Psi(f_\lambda(x)) \in \mathbb{Q}_p(\zeta_p, \zeta_{q-1}), \tag{1.1}$$

where we set $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}^n$.

It can happen that $S(f_\lambda, \mathbf{e}) = 0$ for all $\lambda = (\lambda_1, \ldots, \lambda_N) \in \mathbb{F}_q^N$ (see Eq. (6.2) below). If $S(f_\lambda, \mathbf{e}) \neq 0$ for some λ, then using the method of Ax[5] and Stickelberger's Theorem it is not hard to show (see Eq. (6.3) below) that there is a nonnegative integer C and a polynomial $\hat{H} \in (\mathbb{Q} \cap \mathbb{Z}_p)[\Lambda_1, \ldots, \Lambda_N]$ of degree $\leq q-1$ in each variable and nonzero modulo p, both depending only on A and $\mathbf{e}$, such that

$$S(f_\lambda, \mathbf{e}) \equiv \hat{H}(\omega(\lambda_1), \ldots, \omega(\lambda_N))\pi^C \pmod{\pi^{C+1}}, \tag{1.2}$$

where π is a certain uniformizer for the field $\mathbb{Q}_p(\zeta_p, \zeta_{q-1})$. Let $H(\lambda_1, \ldots, \lambda_N) \in \mathbb{F}_p[\lambda_1, \ldots, \lambda_N]$ be the reduction mod p of $\hat{H}(\omega(\lambda_1), \ldots, \omega(\lambda_N))$. We call $H(\lambda)$ the *Hasse invariant* of the family of exponential sums $S(f_\lambda, \mathbf{e})$. One thus has

$$\operatorname{ord}_p S(f_\lambda, \mathbf{e}) \geq \frac{C}{p-1} \tag{1.3}$$

with equality holding if and only if $H(\lambda_1, \ldots, \lambda_N) \neq 0$, where ord_p denotes the p-adic valuation normalized by $\operatorname{ord}_p p = 1$.

The estimate (1.3) improves on our previous work ([2, Theorem 2], [3, Theorem 3.3]), where the lower bound was expressed in terms of the Newton polyhedron of f_λ. In the case where all multiplicative characters are trivial and f_λ is an ordinary polynomial, estimate (1.3) has already been observed by Moreno, Shum, Castro, and Kumar[15, Theorems 7 and 9], who analyzed $S(f_\lambda, \mathbf{0})$ using the notion of p-degree. These sums over $\mathbb{A}^n$ have been studied further by R. Blache[7, 8, 9]. The notion of p-degree also plays a key role in the proof of our results.

The main point of this article is to show that $H(\lambda)$ is a sum of mod p solutions of certain A-hypergeometric systems. We first show (Sections 2 and 3) that associated to certain lattice points $\gamma \in \mathbb{Z}^n$ are polynomials $F_\gamma(\lambda) \in \mathbb{F}_p[\lambda_1, \ldots, \lambda_N]$ that satisfy A-hypergeometric systems mod p. This generalizes earlier work of Beukers[6]. We then show (Section 6) that associated to $S(f_\lambda, \mathbf{e})$ is a finite set Γ of sequences $(\gamma_0, \gamma_1, \ldots, \gamma_{a-1})$ of these lattice points such that

$$H(\lambda_1, \ldots, \lambda_N) = \sum_{(\gamma_0,\ldots,\gamma_{a-1})\in\Gamma} F_{\gamma_0}(\lambda) F_{\gamma_1}(\lambda^p) \cdots F_{\gamma_{a-1}}(\lambda^{p^{a-1}})$$

(see Theorem 6.6 below for the precise statement). The proof provides an explicit calculation of C and the γ_i in terms of the set A and the vector $\mathbf{e}$ (see Section 6). Using the natural toric decomposition of affine space, the result extends to exponential sums on $\mathbb{A}^n$ as well (see Theorem 7.9). Although not needed in the rest of the article, we describe in Section 4 some relations between the F_γ and truncations of series solutions of A-hypergeometric systems in characteristic 0.

2. A-hypergeometric systems

Let $\mathbb{N}A$ (where $\mathbb{N} = \{0, 1, \ldots\}$) denote the semigroup generated by A and let $\mathbb{Z}A \subseteq \mathbb{Z}^n$ denote the group generated by A. Let $L \subseteq \mathbb{Z}^N$ be the lattice of relations

on A:

$$L = \left\{ l = (l_1, \dots, l_N) \in \mathbb{Z}^N \mid \sum_{i=1}^{N} l_i \mathbf{a}_i = \mathbf{0} \right\}.$$

Let $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{C}^n$. The *$A$-hypergeometric system with parameter β* is the system of partial differential operators in variables $\lambda_1, \dots, \lambda_N$ consisting of the *box operators*

$$\Box_l = \prod_{l_i > 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{l_i} - \prod_{l_i < 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{-l_i} \quad \text{for } l \in L \tag{2.1}$$

and the *Euler* (or *homogeneity*) *operators*

$$Z_i = \sum_{j=1}^{N} a_{ji} \lambda_j \frac{\partial}{\partial \lambda_j} - \beta_i \quad \text{for } i = 1, \dots, n, \tag{2.2}$$

where $\mathbf{a}_j = (a_{j1}, \dots, a_{jn})$. If there is a linear form h on $\mathbb{R}^n$ such that $h(\mathbf{a}_i) = 1$ for $i = 1, \dots, N$, we call this system *nonconfluent*; otherwise, we call it *confluent*.

If the β_i are p-integral rational numbers, one can consider (2.1) and (2.2) modulo p and ask for their solutions in $\mathbb{F}_p((\lambda_1, \dots, \lambda_N))$, the quotient field of the formal power series ring $\mathbb{F}_p[[\lambda_1, \dots, \lambda_N]]$. However, this is not the relevant system for studying exponential sums: one needs the reduction mod p of the p-adically normalized A-hypergeometric system. In [11], Dwork normalized the system corresponding to the Bessel differential equation in order to describe the variation of cohomology of the family of Kloosterman sums over a finite field. Essentially, this normalization guarantees that the p-adic radius of convergence of series solutions is equal to 1. For a more recent example of this see [4], where we extend one of Dwork's results to arbitrary families of exponential sums. The normalization involves simply replacing each λ_i by $\pi\lambda_i$, where $\pi^{p-1} = -p$ (note that π is a uniformizer for the field $\mathbb{Q}_p(\zeta_p, \zeta_{q-1})$). This change of variable has no effect on the Euler operators, however, the box operator $\Box_l$ is transformed to

$$\pi^{-\sum_{l_i>0} l_i} \prod_{l_i > 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{l_i} - \pi^{\sum_{l_i<0} l_i} \prod_{l_i < 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{-l_i}.$$

We then multiply by the smallest power of π that makes both coefficients p-integral:

$$\pi^{\max\{\sum_{l_i>0} l_i, -\sum_{l_i<0} l_i\}} \left(\pi^{-\sum_{l_i>0} l_i} \prod_{l_i > 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{l_i} - \pi^{\sum_{l_i<0} l_i} \prod_{l_i < 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{-l_i} \right).$$

Reducing this expression mod π gives for $l \in L$ the operator

$$\overline{\Box}_l = \begin{cases} \prod_{l_i>0} (\partial/\partial\lambda_i)^{l_i} & \text{if } \sum_{i=1}^N l_i > 0, \\ \prod_{l_i<0} (\partial/\partial\lambda_i)^{-l_i} & \text{if } \sum_{i=1}^N l_i < 0, \\ \prod_{l_i>0} (\partial/\partial\lambda_i)^{l_i} - \prod_{l_i<0} (\partial/\partial\lambda_i)^{-l_i} & \text{if } \sum_{i=1}^N l_i = 0. \end{cases} \tag{2.3}$$

When β is an n-tuple of p-integral rational numbers, one can thus consider two A-hypergeometric systems modulo p: the first consisting of (2.1) and (2.2) and the second consisting of (2.2) and (2.3). It is the second system whose mod p solutions are related to the exponential sums (1.1). However, note that when the system is nonconfluent it is the third possibility in (2.3) that always holds and the two systems mod p are identical.

Let $\beta \in \mathbb{Z}^n$ and set

$$U(\beta) = \left\{ u = (u_1, \ldots, u_N) \in \mathbb{Z}^N \mid \sum_{i=1}^N u_i \mathbf{a}_i = \beta \right\},$$

$$U^+(\beta) = \left\{ u = (u_1, \ldots, u_N) \in \mathbb{N}^N \mid \sum_{i=1}^N u_i \mathbf{a}_i = \beta \right\}.$$

It is clear that $U(\beta) \neq \emptyset$ (resp.: $U^+(\beta) \neq \emptyset$) if and only if $\beta \in \mathbb{Z}A$ (resp.: $\beta \in \mathbb{N}A$). For any nonnegative integer k, put

$$U_k^+(\beta) = \{ u \in U^+(\beta) \mid u_i \leq k \text{ for } i = 1, \ldots, N \}.$$

We define the *weight* of β, $w(\beta)$, to be

$$w(\beta) = \min \left\{ \sum_{i=1}^N u_i \mid u \in U^+(\beta) \right\},$$

and we say that $u \in U^+(\beta)$ is *minimal* if $\sum_{i=1}^N u_i = w(\beta)$. Let $U_{\min}^+(\beta)$ be the subset of minimal elements of $U^+(\beta)$. We say that β is *good* if $U_{\min}^+(\beta) \subseteq U_{p-1}^+(\beta)$ and we say that β is *very good* if $U^+(\beta) = U_{p-1}^+(\beta)$. When β is good (resp.: very good), we can define

$$F_\beta(\lambda_1, \ldots, \lambda_N) = \sum_{u \in U_{\min}^+(\beta)} \frac{\lambda_1^{u_1} \cdots \lambda_N^{u_N}}{u_1! \cdots u_N!} \in \mathbb{F}_p[\lambda_1, \ldots, \lambda_N] \tag{2.4}$$

(resp.:

$$G_\beta(\lambda_1, \ldots, \lambda_N) = \sum_{u \in U^+(\beta)} \frac{\lambda_1^{u_1} \cdots \lambda_N^{u_N}}{u_1! \cdots u_N!} \in \mathbb{F}_p[\lambda_1, \ldots, \lambda_N]). \tag{2.5}$$

For explicit examples of such polynomials, we refer to Example 1 in Section 3 and Example 2 in Section 5.

Let

$$\sigma_A(\beta) = \{ \gamma \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A \mid \gamma \text{ is good} \},$$
$$\tau_A(\beta) = \{ \gamma \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A \mid \gamma \text{ is very good} \}.$$

Both $\sigma_A(\beta)$ and $\tau_A(\beta)$ are finite sets as both are contained in the finite set

$$\left\{ \sum_{i=1}^N c_i \mathbf{a}_i \mid c_i \in \{0, 1, \ldots, p-1\} \text{ for } i = 1, \ldots, N \right\}.$$

Even if $(\beta + p\mathbb{Z}^n) \cap \mathbb{N}A$ is nonempty, the set $\tau_A(\beta)$ may be empty; however,

$$(\beta + p\mathbb{Z}^n) \cap \mathbb{N}A \neq \emptyset \quad \text{implies} \quad \sigma_A(\beta) \neq \emptyset.$$

More precisely, we have the following result.

Lemma 2.6. *Let $\gamma \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A$ be such that $w(\gamma) \leq w(\gamma')$ for all $\gamma' \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A$. Then γ is good.*

Proof. Let $\gamma \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A$ satisfy the hypothesis of the lemma. If $u \in U_{\min}^+(\gamma)$ had $u_i \geq p$ for some i, define $u' = (u'_1, \ldots, u'_N)$ by

$$u'_i = \begin{cases} u_i & \text{if } u_i \leq p-1, \\ u_i - p & \text{if } u_i \geq p, \end{cases}$$

and set $\gamma' = \sum_{i=1}^N u_i'\mathbf{a}_i$. Then $\gamma' \in (\beta + p\mathbb{Z}^n) \cap \mathbb{N}A$ but

$$w(\gamma') \leq \sum_{i=1}^N u_i' < \sum_{i=1}^N u_i = w(\gamma),$$

contradicting the choice of γ. □

Let $S_A(\beta) \subseteq \mathbb{F}_p((\lambda_1, \dots, \lambda_N))$ (resp.: $T_A(\beta)$) be the solution space of the mod p A-hypergeometric system (2.2), (2.3) (resp.: (2.1), (2.2)). Since differential operators in characteristic p annihilate all p-th powers, we consider $S_A(\beta)$ and $T_A(\beta)$ as vector spaces over the field $\mathbb{F}_p((\lambda_1^p, \dots, \lambda_N^p))$.

The following result is a slight generalization of Beukers[6, Proposition 4.1]. Although it is not needed for this article, we include it to provide some context for the results of the next section.

Theorem 2.7. *The set of polynomials $\{G_\gamma \mid \gamma \in \tau_A(\beta)\}$ is a basis for $T_A(\beta)$.*

Sketch of proof. One can repeat the argument of [6]. Although Beukers makes an overriding assumption that his system is nonconfluent, that hypothesis is not used in the part of his paper dealing with mod p solutions. He also assumes that $\mathbb{N}A$ equals the set of all lattice points in the real cone generated by A, a condition that is needed in the proof of [6, Proposition 4.1]. Using our set of solutions $\{G_\gamma\}_{\gamma\in\tau_A(\beta)}$ in place of his, the proof of [6, Proposition 4.1] remains valid in the unsaturated case. (In the saturated case, our set of solutions is identical to the one constructed by Beukers.) □

3. Mod p solutions

The main purpose of this section is to prove the following result.

Theorem 3.1. *The set of polynomials $\{F_\gamma \mid \gamma \in \sigma_A(\beta)\}$ is a basis for $S_A(\beta)$.*

Proof. We first show that each F_γ is a solution of the system (2.2), (2.3). The definition of $\sigma_A(\beta)$ implies that F_γ satisfies Equations (2.2) modulo p, so it remains to show that F_γ is a mod p solution of the box operators (2.3). Fix $l = (l_1, \dots, l_N)$ satisfying $\sum_{i=1}^N l_i\mathbf{a}_i = \mathbf{0}$. First suppose that $\sum_{i=1}^N l_i > 0$. We must show that

$$\prod_{l_i>0} \left(\frac{\partial}{\partial\lambda_i}\right)^{l_i} (\lambda_1^{u_1}\cdots\lambda_N^{u_N}) = 0 \quad \text{for all } u \in U^+_{\min}(\gamma). \tag{3.2}$$

Fix $u \in U^+_{\min}(\gamma)$ and consider $v \in \mathbb{Z}^N$ defined by $v_i = u_i - l_i$ for $i = 1, \dots, N$. Then we have

$$\sum_{i=1}^N v_i\mathbf{a}_i = \sum_{i=1}^N u_i\mathbf{a}_i - \sum_{i=1}^N l_i\mathbf{a}_i = \gamma$$

and

$$\sum_{i=1}^N v_i = \sum_{i=1}^N u_i - \sum_{i=1}^N l_i < \sum_{i=1}^N u_i = w(\gamma).$$

If $v_i \geq 0$ for all i, we would have $v \in U^+(\gamma)$ with $\sum_{i=1}^N v_i < \sum_{i=1}^N u_i$, contradicting $u \in U^+_{\min}(\gamma)$. It follows that $v_i < 0$ for some i. But $u_i \geq 0$ for all i implies $u_i - l_i \geq 0$ if $l_i \leq 0$, so we must have $u_i - l_i < 0$ for some $l_i > 0$. This immediately implies (3.2).

The proof is similar if $\sum_{i=1}^N l_i < 0$ so suppose that $\sum_{i=1}^N l_i = 0$. We must show that

$$\left(\prod_{l_i>0}\left(\frac{\partial}{\partial\lambda_i}\right)^{l_i} - \prod_{l_i<0}\left(\frac{\partial}{\partial\lambda_i}\right)^{-l_i}\right)\left(\sum_{u\in U^+_{\min}(\gamma)}\frac{\lambda_1^{u_1}\cdots\lambda_N^{u_N}}{u_1!\cdots u_N!}\right) = 0. \tag{3.3}$$

Write $l = l_+ - l_-$, where $l_+ = (l_1^+,\dots,l_N^+)$ and $l_- = (l_1^-,\dots,l_N^-)$ are defined by

$$l_i^+ = \max\{l_i, 0\},\quad l_i^- = \max\{-l_i, 0\}.$$

Let

$$U_1(\gamma) = \{u\in U^+_{\min}(\gamma) \mid u_i - l_i \geq 0 \text{ for } i = 1,\dots,N\},$$
$$U_2(\gamma) = \{v\in U^+_{\min}(\gamma) \mid v_i + l_i \geq 0 \text{ for } i = 1,\dots,N\}.$$

Then we have

$$\prod_{l_i>0}\left(\frac{\partial}{\partial\lambda_i}\right)^{l_i}(F_\gamma) = \sum_{u\in U_1(\gamma)}\frac{\lambda_1^{u_1-l_1^+}\cdots\lambda_N^{u_N-l_N^+}}{(u_1-l_1^+)!\cdots(u_N-l_N^+)!}, \tag{3.4}$$

$$\prod_{l_i<0}\left(\frac{\partial}{\partial\lambda_i}\right)^{-l_i}(F_\gamma) = \sum_{v\in U_2(\gamma)}\frac{\lambda_1^{v_1-l_1^-}\cdots\lambda_N^{v_N-l_N^-}}{(v_1-l_1^-)!\cdots(v_N-l_N^-)!}. \tag{3.5}$$

Note that we have a one-to-one correspondence between the sets $U_1(\gamma)$ and $U_2(\gamma)$: if $u\in U_1(\gamma)$, then $v = u - l\in U_2(\gamma)$. The inverse of this map is given by: send $v\in U_2(\gamma)$ to $v + l\in U_1(\gamma)$. Furthermore, if $u\in U_1(\gamma)$ and $v\in U_2(\gamma)$ are related under this correspondence, then

$$u_i - l_i^+ = v_i - l_i^- \quad \text{for } i = 1,\dots,N.$$

This shows that the right-hand sides of (3.4) and (3.5) are equal, and (3.3) follows immediately. We have established that F_γ is a solution of the system (2.2), (2.3).

The functions $\{F_\gamma\}_{\gamma\in\sigma_A(\beta)}$ are polynomials in $\lambda_1,\dots,\lambda_N$ of degree $\leq p-1$ in each variable and the sets $\{U^+_{\min}(\gamma)\}_{\gamma\in\sigma_A(\beta)}$ are mutually disjoint, hence the set $\{F_\gamma\}_{\gamma\in\sigma_A(\beta)}$ is linearly independent over $\mathbb{F}_p((\lambda_1^p,\dots,\lambda_N^p))$. It remains to show that every solution of (2.2), (2.3) is an $\mathbb{F}_p((\lambda_1^p,\dots,\lambda_N^p))$-linear combination of these polynomials.

Let G be any solution of (2.2), (2.3) in $\mathbb{F}_p((\lambda_1,\dots,\lambda_N))$. Then G is a (possibly infinite) sum of expressions of the form $\lambda_1^{pk_1}\cdots\lambda_N^{pk_N}G_{k_1\dots k_N}$ ($k_1,\dots,k_N\in\mathbb{Z}$), where $G_{k_1\dots k_N}$ is a polynomial of degree $\leq p-1$ in each variable $\lambda_1,\dots,\lambda_N$. Furthermore, G is a solution of (2.2), (2.3) if and only if each $G_{k_1\dots k_N}$ is. So we may take G to be a polynomial of degree $\leq p-1$ in each variable. To satisfy (2.2), each monomial $\lambda_1^{k_1}\cdots\lambda_N^{k_N}$ in G must satisfy

$$\sum_{i=1}^N k_i\mathbf{a}_i \equiv \beta \pmod{p\mathbb{Z}^n}.$$

It follows that we may write

$$G = \sum_{j=1}^J\sum_{u\in U^+_{p-1}(\gamma_j)} c_u\lambda_1^{u_1}\cdots\lambda_N^{u_N},$$

where $\gamma_1, \dots, \gamma_J \equiv \beta \pmod{p\mathbb{Z}^n}$. Put

$$G_{\gamma_j} = \sum_{u \in U^+_{p-1}(\gamma_j)} c_u \lambda_1^{u_1} \cdots \lambda_N^{u_N}.$$

Each G_{γ_j} satisfies (2.2). Suppose $l \in L$ and $\sum_{i=1}^N l_i > 0$. The corresponding box operator,

$$\overline{\Box}_l = \prod_{l_i > 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{l_i},$$

annihilates G if and only if it annihilates each monomial in G; so it annihilates G if and only if it annihilates each G_{γ_j}. A similar argument applies when $\sum_{i=1}^N l_i < 0$, so assume $\sum_{i=1}^N l_i = 0$. The corresponding box operator is

$$\overline{\Box}_l = \prod_{l_i > 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{l_i} - \prod_{l_i < 0} \left(\frac{\partial}{\partial \lambda_i} \right)^{-l_i}.$$

It is straightforward to check that the monomials appearing in the $\overline{\Box}_l(G_{\gamma_j})$ form disjoint sets for $j = 1, \dots, J$. It follows that G satisfies (2.3) if and only if each G_{γ_j} does.

We are finally reduced to the case where

$$G = \sum_{u \in U^+_{p-1}(\gamma)} c_u \lambda_1^{u_1} \cdots \lambda_N^{u_N}$$

for some $\gamma \equiv \beta \pmod{p\mathbb{Z}^n}$. We claim that $c_u = 0$ if $u \notin U^+_{\min}(\gamma)$. Pick $v \in U^+_{\min}(\gamma)$ and take $l = u - v \in L$. If $u \notin U^+_{\min}(\gamma)$, then $\sum_{i=1}^N u_i - v_i > 0$, so the corresponding box operator is

$$\overline{\Box}_l = \prod_{u_i > v_i} \left(\frac{\partial}{\partial \lambda_i} \right)^{u_i - v_i}.$$

Since $u_i - v_i \leq u_i$ for all i, it is clear that $\overline{\Box}_l(c_u \lambda_1^{u_1} \cdots \lambda_N^{u_N}) \neq 0$ unless $c_u = 0$.

We now have

$$G = \sum_{u \in U^+_{p-1}(\gamma) \cap U^+_{\min}(\gamma)} c_u \lambda_1^{u_1} \cdots \lambda_N^{u_N}, \tag{3.6}$$

and we need to show that $G = 0$ unless γ is good (i.e., $U^+_{\min}(\gamma) \subseteq U^+_{p-1}(\gamma)$), and that when γ is good, G is a scalar multiple of the function F_γ defined earlier. If $U^+_{p-1}(\gamma) \cap U^+_{\min}(\gamma) = \emptyset$ then $G = 0$. If $U^+_{\min}(\gamma)$ is a singleton, then either $U^+_{\min}(\gamma) \subseteq U^+_{p-1}(\gamma)$ (so γ is good and G is clearly a scalar multiple of F_γ) or $U^+_{p-1}(\gamma) \cap U^+_{\min}(\gamma) = \emptyset$ (so $G = 0$).

So suppose $U^+_{\min}(\gamma)$ has at least two elements and $U^+_{p-1}(\gamma) \cap U^+_{\min}(\gamma) \neq \emptyset$. Let $u \in U^+_{p-1}(\gamma) \cap U^+_{\min}(\gamma)$ and let $v \in U^+_{\min}(\gamma)$ (for notational convenience, we set $c_v = 0$ if $v \notin U^+_{p-1}(\gamma)$). Put $l = u - v \in L$. Since $\sum_{i=1}^N u_i - v_i = 0$, the corresponding box operator is

$$\overline{\Box}_l = \prod_{u_i > v_i} \left(\frac{\partial}{\partial \lambda_i} \right)^{u_i - v_i} - \prod_{u_i < v_i} \left(\frac{\partial}{\partial \lambda_i} \right)^{v_i - u_i}.$$

The coefficient of $\prod_{i=1}^N \lambda_i^{\min\{u_i,v_i\}}$ in $\overline{\Box}_l(G)$ is

$$c_u \prod_{u_i>v_i} u_i(u_i-1)\cdots(v_i+1) - c_v \prod_{u_i<v_i} v_i(v_i-1)\cdots(u_i+1). \tag{3.7}$$

Since $u_i \leq p-1$ for $i=1,\dots,N$, the coefficient of c_u in this expression is $\neq 0$. If γ is not good, then there exists $v \in U^+_{\min}(\gamma)$ such that $v \notin U^+_{p-1}(\gamma)$. Since $c_v = 0$ and since $\overline{\Box}_l(G) = 0$ implies the vanishing of (3.7), it follows that $c_u = 0$. Since u was an arbitrary element of $U^+_{p-1}(\gamma)\cap U^+_{\min}(\gamma)$, we conclude that $G = 0$. If γ is good, then $U^+_{\min}(\gamma) \subseteq U^+_{p-1}(\gamma)$, so the sum in (3.6) is over $U^+_{\min}(\gamma)$. If $u,v \in U^+_{\min}(\gamma)$, then the coefficients of c_u and c_v in (3.7) are both $\neq 0$. Equation (3.7) and the vanishing of $\overline{\Box}_l(G)$ then imply that the value of c_u for one $u \in U^+_{\min}(\gamma)$ determines the values of c_v for all $v \in U^+_{\min}(\gamma)$. This proves that the space of solutions of the form (3.6) is one-dimensional, hence G is a scalar multiple of F_γ. $\Box$

Example 1: Let $A = \{\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3,\mathbf{a}_4\} \subseteq \mathbb{Z}^3$, where $\mathbf{a}_1 = (1,0,0)$, $\mathbf{a}_2 = (0,1,0)$, $\mathbf{a}_3 = (0,0,1)$, and $\mathbf{a}_4 = (1,1,-1)$. Then $(-1/2,-1/2,0)$ is p-integral for any odd prime p and taking $\beta = ((p-1)/2,(p-1)/2,0) \in \mathbb{Z}^3$ we have $\beta \equiv (-1/2,-1/2,0) \pmod{p}$. The nonnegative integer solutions of the system of equations

$$\sum_{i=1}^4 c_i\mathbf{a}_i = \left(\frac{p-1}{2},\frac{p-1}{2},0\right)$$

are given by

$$c_1 = c_2 = \frac{p-1}{2} - l, \quad c_3 = c_4 = l, \quad \text{for } l = 0,1,\dots,\frac{p-1}{2}.$$

We thus have $U^+(\beta) = U^+_{p-1}(\beta) = U^+_{\min}(\beta)$, $w(\beta) = p-1$, and

$$U^+_{\min}(\beta) = \left\{\left(\frac{p-1}{2}-l,\frac{p-1}{2}-l,l,l\right) \mid l \in \{0,1,\dots,(p-1)/2\}\right\}.$$

In particular, β is very good and

$$F_\beta(\lambda) = \sum_{l=0}^{(p-1)/2} \frac{\lambda_1^{(p-1)/2-l}\lambda_2^{(p-1)/2-l}\lambda_3^l\lambda_4^l}{((p-1)/2-l)!^2\, l!^2}.$$

This can be simplified by multiplying by $(-1)^{(p+1)/2}((p-1)/2)!^2$ ($\equiv 1 \pmod{p}$) to give

$$F_\beta(\lambda) = -(-\lambda_1\lambda_2)^{(p-1)/2} \sum_{l=0}^{(p-1)/2} \binom{(p-1)/2}{l}^2 \left(\frac{\lambda_3\lambda_4}{\lambda_1\lambda_2}\right)^l.$$

4. Mod p solutions and A-hypergeometric series

The results of this section are not needed elsewhere in this paper, however, we include them with a view to future applications.

Fix $\beta \in \mathbb{Z}^n$ for which $(\beta + p\mathbb{Z}^n)\cap \mathbb{N}A \neq \emptyset$. By Lemma 2.6 we may choose $\gamma \in (\beta + p\mathbb{Z}^n)\cap\mathbb{N}A$ to be good. Consider the associated solution

$$F_\gamma(\lambda) = \sum_{u\in U^+_{\min}(\gamma)} \frac{\lambda_1^{u_1}\cdots\lambda_N^{u_N}}{u_1!\cdots u_N!}$$

of the mod p system (2.2), (2.3). We shall compare F_γ with a formal solution of the A-hypergeometric system in characteristic 0 consisting of the operators

$$\sum_{j=1}^{N} a_{ji}\lambda_j \frac{\partial}{\partial \lambda_j} - \frac{\gamma}{1-p} \quad \text{for } i = 1, \ldots, n \tag{4.1}$$

and

$$\pi^{-\sum_{l_i>0} l_i} \prod_{l_i>0} \left(\frac{\partial}{\partial \lambda_i}\right)^{l_i} - \pi^{\sum_{l_i<0} l_i} \prod_{l_i<0} \left(\frac{\partial}{\partial \lambda_i}\right)^{-l_i} \quad \text{for } l \in L. \tag{4.2}$$

Fix an element $u^{(0)} \in U^+_{\min}(\gamma)$ and define $v^{(0)} = u^{(0)}/(1-p)$. Then we have

$$\sum_{i=1}^{N} v_i^{(0)} \mathbf{a}_i = \frac{\gamma}{1-p} \tag{4.3}$$

and, since γ is good, we have

$$-1 \leq v_i^{(0)} \leq 0 \quad \text{for } i = 1, \ldots, N.$$

Recall that the *negative support* of a vector $x = (x_1, \ldots, x_N) \in \mathbb{C}^N$ is defined as $\text{nsupp}(x) = \{i \in \{1, \ldots, N\} \mid x_i \in \mathbb{Z}_{<0}\}$. We make the hypothesis that $v^{(0)}$ has minimal negative support in the sense of [16, Section 3.4], i.e., that there is no element $l \in L$ such that $\text{nsupp}(v^{(0)} + l)$ is a proper subset of $\text{nsupp}(v^{(0)})$. Put

$$N_{v^{(0)}} = \{l \in L \mid \text{nsupp}(v^{(0)} + l) = \text{nsupp}(v^{(0)})\}.$$

Since Eq. (4.2) is obtained from the usual box operators by replacing each variable λ_i by $\pi\lambda_i$, this implies (see [16, Proposition 3.4.13]) that the formal series

$$\phi_{v^{(0)}}(\lambda) = \sum_{l \in N_{v^{(0)}}} \frac{[v^{(0)}]_{l_-}}{[v^{(0)} + l]_{l_+}} (\pi\lambda)^{v^{(0)}+l} \tag{4.4}$$

is a solution of the system (4.1), (4.2), where

$$[v^{(0)}]_{l_-} = \prod_{l_i<0} \prod_{j=1}^{-l_i} (v_i^{(0)} - j + 1)$$

and

$$[v^{(0)} + l]_{l_+} = \prod_{l_i>0} \prod_{j=1}^{l_i} (v_i^{(0)} + j).$$

Note that

$$(\pi\lambda)^{-pv^{(0)}} \phi_{v^{(0)}}(\lambda) = \sum_{l \in N_{v^{(0)}}} \frac{[v^{(0)}]_{l_-}}{[v^{(0)} + l]_{l_+}} (\pi\lambda)^{u^{(0)}+l}$$

is a formal series where all powers of λ lie in $\mathbb{Z}^N$. Let $G_{v^{(0)}}(\lambda) \in \mathbb{Q}[\pi][\lambda]$ denote the truncation of $(\pi\lambda)^{-pv^{(0)}} \phi_{v^{(0)}}(\lambda)$ obtained by eliminating all terms except those containing monomials $\lambda_1^{j_1} \cdots \lambda_N^{j_N}$ satisfying $0 \leq j_i \leq p-1$ for $i = 1, \ldots, N$. More precisely, if we let

$$N'_{v^{(0)}} = \{l \in N_{v^{(0)}} \mid u^{(0)} + l \in U^+_{p-1}(\gamma)\},$$

then

$$G_{v^{(0)}}(\lambda) = \sum_{l\in N'_{v^{(0)}}} \frac{[v^{(0)}]_{l_-}}{[v^{(0)}+l]_{l_+}}(\pi\lambda)^{u^{(0)}+l}. \tag{4.5}$$

Proposition 4.6. *If $v^{(0)}$ has minimal negative support, then $\pi^{-w(\gamma)}G_{v^{(0)}}(\lambda)$ has p-integral coefficients and*

$$\pi^{-w(\gamma)}G_{v^{(0)}}(\lambda) \equiv (u_1^{(0)}!)\cdots(u_N^{(0)}!)F_\gamma(\lambda) \pmod{\pi}.$$

Proof. Suppose that $u^{(0)}+l\in U^+(\gamma)$. We claim that $l\in N_{v^{(0)}}$. Suppose that for some i, $v_i^{(0)}+l_i\in\mathbb{Z}_{<0}$ but $v_i^{(0)}\notin\mathbb{Z}_{<0}$. Then we must have $v_i^{(0)}=0$ and $l_i<0$. But $v_i^{(0)}=0$ implies $u_i^{(0)}=0$ so $u_i^{(0)}+l_i<0$, contradicting $u^{(0)}+l\in U^+(\gamma)$. It follows that $\mathrm{nsupp}(v^{(0)}+l)\subseteq\mathrm{nsupp}(v^{(0)})$, and they must be equal since $v^{(0)}$ is assumed to have minimal negative support.

It follows that $N'_{v^{(0)}}=\{l\in L\mid u^{(0)}+l\in U^+_{p-1}(\gamma)\}$. We can thus write $G_{v^{(0)}}(\lambda)$ as the sum of two polynomials $G_1(\lambda)$ and $G_2(\lambda)$, where $G_1(\lambda)$ is the sum of those terms on the right-hand side of (4.5) with $u^{(0)}+l\in U^+_{\min}(\gamma)$ and $G_2(\lambda)$ is the sum of those terms with $u^{(0)}+l\in U^+_{p-1}(\gamma)\setminus U^+_{\min}(\gamma)$. We shall establish the proposition by showing that both $\pi^{-w(\gamma)}G_1(\lambda)$ and $\pi^{-w(\gamma)}G_2(\lambda)$ have p-integral coefficients and that

$$\pi^{-w(\gamma)}G_2(\lambda)\equiv 0 \pmod{\pi}, \tag{4.7}$$

$$\pi^{-w(\gamma)}G_1(\lambda)\equiv (u_1^{(0)}!)\cdots(u_N^{(0)}!)F_\gamma(\lambda) \pmod{\pi}. \tag{4.8}$$

Note that in the p-adic integers $\mathbb{Z}_p$ we have the equality

$$v_i^{(0)} = u_i^{(0)} + u_i^{(0)}p + u_i^{(0)}p^2+\cdots. \tag{4.9}$$

If $l\in N'_{v^{(0)}}$ has $l_i\geq 0$, then $u_i^{(0)}+l_i\leq p-1$ implies $l_i\leq p-1-u_i^{(0)}$. It then follows from (4.9) that $\prod_{j=1}^{l_i}(v_i^{(0)}+j)$ is a p-adic unit, hence $[v^{(0)}+l]_{l_+}$ is a p-adic unit. If $l\in N'_{v^{(0)}}$ has $l_i<0$, then $u_i^{(0)}+l_i\geq 0$ implies $l_i\geq -u_i^{(0)}$. It follows from (4.9) that $\prod_{j=1}^{-l_i}(v_i^{(0)}-j+1)$ is a p-adic unit, hence $[v^{(0)}]_{l_-}$ is a p-adic unit. This proves that the coefficient of $\lambda^{u^{(0)}+l}$ in $G_{v^{(0)}}(\lambda)$ is p-integral and divisible by $\pi^{\sum_{i=1}^N u_i^{(0)}+l_i}$. If $u^{(0)}+l\notin U^+_{\min}(\gamma)$, then $\sum_{i=1}^N u_i^{(0)}+l_i>w(\gamma)$, which establishes (4.7). To prove (4.8), we must show that for $u^{(0)}+l\in U^+_{\min}(\gamma)$,

$$\frac{[v^{(0)}]_{l_-}}{[v^{(0)}+l]_{l_+}} \equiv \frac{(u_1^{(0)}!)\cdots(u_N^{(0)}!)}{(u_1^{(0)}+l_1)!\cdots(u_N^{(0)}+l_N)!} \pmod{p}. \tag{4.10}$$

If $l_i<0$, then by (4.9)

$$\begin{aligned}\prod_{j=1}^{-l_i}(v_i^{(0)}-j+1) &\equiv \prod_{j=1}^{-l_i}(u_i^{(0)}-j+1) \pmod{p}\\ &= \frac{u_i^{(0)}!}{(u_i^{(0)}+l_i)!},\end{aligned}$$

and if $l_i > 0$, then by (4.9)

$$\prod_{j=1}^{l_i}(v_i^{(0)}+j) \equiv \prod_{j=1}^{l_i}(u_i^{(0)}+j) \pmod p$$
$$= \frac{(u_i^{(0)}+l_i)!}{u_i^{(0)}!}.$$

These congruences imply (4.8). Note that the coefficients of $\pi^{-w(\gamma)}G_1(\lambda)$ lie in $\mathbb{Q}\cap\mathbb{Z}_p$, so (4.8) is actually a congruence mod p. □

Example 1(cont.): We maintain the notation of Example 1 from the previous section. The lattice L is given by $L = \{(-l,-l,l,l) \mid l \in \mathbb{Z}\}$. Choose $u^{(0)} = ((p-1)/2,(p-1)/2,0,0)$, so that $v^{(0)} = (-1/2,-1/2,0,0)$. Then $v^{(0)}$ has minimal negative support and the solution (4.4) of the system (4.1), (4.2) (with $\gamma/(1-p) = (-1/2,-1/2,0)$) is (using the Pochhammer notation $(x)_l = x(x+1)\cdots(x+l-1)$)

$$\phi_{v^{(0)}}(\lambda) = \pi^{-1}\lambda_1^{-1/2}\lambda_2^{-1/2}\sum_{l=0}^{\infty}\left(\left(\frac{1}{2}\right)_l\Big/ l\,!\right)^2\left(\frac{\lambda_3\lambda_4}{\lambda_1\lambda_2}\right)^l.$$

This gives

$$(\pi\lambda)^{-pv^{(0)}}\phi_{v^{(0)}}(\lambda) = \pi^{p-1}\lambda_1^{(p-1)/2}\lambda_2^{(p-1)/2}\sum_{l=0}^{\infty}\left(\left(\frac{1}{2}\right)_l\Big/ l\,!\right)^2\left(\frac{\lambda_3\lambda_4}{\lambda_1\lambda_2}\right)^l,$$

hence

$$G_{v^{(0)}}(\lambda) = \pi^{p-1}(\lambda_1\lambda_2)^{(p-1)/2}\sum_{l=0}^{(p-1)/2}\left(\left(\frac{1}{2}\right)_l\Big/ l\,!\right)^2\left(\frac{\lambda_3\lambda_4}{\lambda_1\lambda_2}\right)^l.$$

The assertion of Proposition 4.6 thus reduces to the congruence (see the formula for $F_\gamma(\lambda)$ in Example 1)

$$(\lambda_1\lambda_2)^{(p-1)/2}\sum_{l=0}^{(p-1)/2}\left(\left(\frac{1}{2}\right)_l\Big/ l\,!\right)^2\left(\frac{\lambda_3\lambda_4}{\lambda_1\lambda_2}\right)^l \equiv$$
$$((p-1)/2)!^2\sum_{l=0}^{(p-1)/2}\frac{\lambda_1^{(p-1)/2-l}\lambda_2^{(p-1)/2-l}\lambda_3^l\lambda_4^l}{(\frac{p-1}{2}-l)!^2\, l!^2}.$$

Remark: It would be interesting to know when the coefficients of the series (4.4) are p-integral, as they are in this example (except for the factor π^{-1}).

5. The p-weight of a set of lattice points

Fix $q = p^a$. In Section 3 we showed that good lattice points correspond to mod p solutions of an A-hypergeometric system. In this section we show that lattice points minimizing the "p-weight" of a set of lattice points satisfying condition (5.5) below give rise to sequences of length a of good lattice points (Proposition 5.6 below).

Let $U_{q-1}^+ = \{u = (u_1,\dots,u_N) \mid 0 \le u_i \le q-1 \text{ for } i = 1,\dots,N\}$. For each $u \in U_{q-1}^+$, we define $u^{(0)},\dots,u^{(a-1)} \in \{0,1,\dots,p-1\}^N$, $u^{(k)} = (u_1^{(k)},\dots,u_N^{(k)})$, by writing

$$u_i = u_i^{(0)} + u_i^{(1)}p + \cdots + u_i^{(a-1)}p^{a-1} \quad \text{for } i = 1,\dots,N \tag{5.1}$$

and we define

$$\gamma_k = \sum_{i=1}^{N} u_i^{(k)} \mathbf{a}_i \quad \text{for } k = 0, \dots, a-1. \tag{5.2}$$

Note that

$$\sum_{k=0}^{a-1} p^k \gamma_k = \sum_{i=1}^{N} u_i \mathbf{a}_i. \tag{5.3}$$

Define the *p-weight* of u, $w_p(u)$, to be

$$w_p(u) = \sum_{i=1}^{N} \sum_{k=0}^{a-1} u_i^{(k)}.$$

Note that since $w(\gamma_k) \leq \sum_{i=1}^{N} u_i^{(k)}$ with equality holding if and only if $u^{(k)} \in U^+_{\min}(\gamma_k)$ we have

$$w_p(u) \geq \sum_{k=0}^{a-1} w(\gamma_k), \tag{5.4}$$

with equality holding if and only if $u^{(k)} \in U^+_{\min}(\gamma_k)$ for all k.

Let $M \subseteq \mathbb{Z}^n$ be a subset satisfying the condition: For $\mathbf{a} = \sum_{i=1}^{N} c_i \mathbf{a}_i \in \mathbb{N}A$,

$$\text{if } \mathbf{a} \in M \text{ and } c_{i_0} \geq q \text{ for some } i_0, \text{ then } \mathbf{a} - (q-1)\mathbf{a}_{i_0} \in M \tag{5.5}$$

and let $U_M = \{u \in U^+_{q-1} \mid \sum_{i=1}^{N} u_i \mathbf{a}_i \in M\}$. (In the next section we shall apply the results of this section taking $M = \mathbf{e} + (q-1)\mathbb{Z}^n$ for a certain choice of $\mathbf{e} \in \mathbb{Z}^n$.) We assume for the remainder of this section that $U_M \neq \emptyset$ and we define the *p-weight* of M, $w_p(M)$, by

$$w_p(M) = \min\{w_p(u) \mid u \in U_M\}.$$

Put $U_{M,\min} = \{u \in U_M \mid w_p(u) = w_p(M)\}$. The main result of this section is the following assertion.

Proposition 5.6. *Let $u \in U_{M,\min}$ and let $\{u^{(k)}\}_{k=0}^{a-1}$ and $\{\gamma_k\}_{k=0}^{a-1}$ be defined by* (5.1) *and* (5.2)*, respectively. Then for $k = 0, \dots, a-1$, γ_k is good and $u^{(k)} \in U^+_{\min}(\gamma_k)$.*

Proof. Let $u \in U_{M,\min}$ and suppose that γ_{k_1} is not good. Then there exists $v^{(k_1)} \in U^+_{\min}(\gamma_{k_1})$ with $v_{i_1}^{(k_1)} \geq p$ for some i_1. For $k \neq k_1$ define $v^{(k)} = u^{(k)}$ and set $v = (v_1, \dots, v_N)$, where

$$v_i = \sum_{k=0}^{a-1} v_i^{(k)} p^k \quad \text{for } i = 1, \dots, N.$$

Note that

$$\sum_{i=1}^{N} v_i \mathbf{a}_i = \sum_{k=0}^{a-1} \left(\sum_{i=1}^{N} v_i^{(k)} p^k \right) \mathbf{a}_i = \sum_{k=0}^{a-1} p^k \gamma_k = \sum_{i=1}^{N} u_i \mathbf{a}_i \in M \tag{5.7}$$

and that (since $\sum_{i=1}^{N} v_i^{(k_1)} \leq \sum_{i=1}^{N} u_i^{(k_1)}$)

$$\sum_{i=1}^{N} \sum_{k=0}^{a-1} v_i^{(k)} \leq w_p(u) = w_p(M). \tag{5.8}$$

Suppose first that $k_1 < a-1$. Define

$$
\begin{cases} w_i^{(k)} = v_i^{(k)} & \text{if } k \neq k_1, k_1+1 \text{ or if } i \neq i_1, \\ w_{i_1}^{(k_1)} = v_{i_1}^{(k_1)} - p, \\ w_{i_1}^{(k_1+1)} = v_{i_1}^{(k_1+1)} + 1, \end{cases} \tag{5.9}
$$

and put

$$
w_i = \sum_{k=0}^{a-1} w_i^{(k)} p^k \quad \text{for } i = 1, \ldots, N.
$$

With this definition we have $w_i = v_i$ for $i = 1, \ldots, N$, so (5.7) implies

$$
\sum_{i=1}^{N} w_i \mathbf{a}_i = \sum_{i=1}^{N} u_i \mathbf{a}_i \in M.
$$

If $k_1 = a-1$, replace k_1+1 by 0 in formula (5.9). We have $v_{i_1}^{(a-1)} \geq p$, so $v_{i_1} \geq q$. By (5.9), $w_i = v_i$ for $i \neq i_1$ while $w_{i_1} = v_{i_1} - (q-1)$, so in this case (5.7) implies

$$
\sum_{i=1}^{N} w_i \mathbf{a}_i = -(q-1)\mathbf{a}_{i_1} + \sum_{i=1}^{N} v_i \mathbf{a}_i \in M
$$

by condition (5.5). Thus in both cases we have $\sum_{i=1}^{N} w_i \mathbf{a}_i \in M$.

If $w_{i_2}^{(k_2)} \geq p$ for some k_2, i_2, we may repeat the reduction step (5.9). After finitely many steps we arrive at $\tilde{w}$ with $\tilde{w}_i^{(k)} \leq p-1$ for all k and i and $\sum_{i=1}^{N} \tilde{w}_i \mathbf{a}_i \in M$, hence $\tilde{w} \in U_M$. But by the construction of $\tilde{w}$ and Eq. (5.8) we have

$$
w_p(\tilde{w}) = \sum_{i=1}^{N} \sum_{k=0}^{a-1} \tilde{w}_i^{(k)} < \sum_{i=1}^{N} \sum_{k=0}^{a-1} v_i^{(k)} \leq w_p(u) = w_p(M).
$$

This contradicts the definition of $w_p(M)$, so γ_k must be good for all k.

It remains to show that $u^{(k)} \in U^+_{\min}(\gamma_k)$ for all k. For each k choose $v^{(k)} \in U^+_{\min}(\gamma_k)$. Since γ_k is good we have $0 \leq v_i^{(k)} \leq p-1$ for all i and k. Define

$$
v_i = \sum_{k=0}^{a-1} v_i^{(k)} p^k \quad \text{for } i = 1, \ldots, N.
$$

Then $0 \leq v_i \leq q-1$ for all i and

$$
\sum_{i=1}^{N} v_i \mathbf{a}_i = \sum_{k=0}^{a-1} \left(\sum_{i=1}^{N} v_i^{(k)} p^k \right) \mathbf{a}_i = \sum_{k=0}^{a-1} p^k \gamma_k = \sum_{i=1}^{N} u_i \mathbf{a}_i,
$$

so $v \in U_M$. Since $v^{(k)} \in U^+_{\min}(\gamma_k)$ for all k, we have equality holding in (5.4) for v:

$$
w_p(v) = \sum_{k=0}^{a-1} w(\gamma_k).
$$

We thus have

$$
w_p(v) = \sum_{k=0}^{a-1} w(\gamma_k) \leq \sum_{k=0}^{a-1} \left(\sum_{i=1}^{N} u_i^{(k)} \right) = w_p(u). \tag{5.10}
$$

Since $u \in U_{M,\min}$, it follows that $v \in U_{M,\min}$ also and that equality holds in (5.10). In particular, we must have $w(\gamma_k) = \sum_{i=1}^N u_i^{(k)}$, i.e., $u^{(k)} \in U^+_{\min}(\gamma_k)$, for all k. This completes the proof of Proposition 5.6. $\square$

In summary, we have proved that every $u \in U_{M,\min}$ gives rise (by (5.1) and (5.2)) to sequences $(u^{(0)}, \dots, u^{(a-1)})$ and $(\gamma_0, \dots, \gamma_{a-1})$, with γ_k good and $u^{(k)} \in U^+_{\min}(\gamma_k)$ for all k, such that (by Eq. (5.3))

$$\sum_{k=0}^{a-1} p^k \gamma_k \in M. \tag{5.11}$$

Furthermore, equality holds in (5.4), so

$$w_p(M) = \sum_{k=0}^{a-1} w(\gamma_k). \tag{5.12}$$

Conversely, suppose we are given a sequence $(\gamma_0, \dots, \gamma_{a-1}) \in (\mathbb{Z}^n)^a$, all γ_k good, satisfying (5.11) and (5.12). Choose $u^{(k)} \in U^+_{\min}(\gamma_k)$ for $k = 0, \dots, a-1$ and define $u \in \mathbb{N}^N$ by the formula

$$u_i = \sum_{k=0}^{a-1} u_i^{(k)} p^k \quad \text{for } i = 1, \dots, N. \tag{5.13}$$

Since all γ_k are good we have $0 \leq u_i^{(k)} \leq p-1$ for all k and i, which implies that $u \in U^+_{q-1}$. Eq. (5.11) implies that $u \in U_M$ and Eq. (5.12) implies that $u \in U_{M,\min}$.

It follows that we can decompose the set $U_{M,\min}$ as follows. Let Γ_M be the set of all sequences $(\gamma_0, \dots, \gamma_{a-1})$ of good elements of $\mathbb{Z}^n$ satisfying (5.11) and (5.12). For $(\gamma_0, \dots, \gamma_{a-1}) \in \Gamma_M$, let $U(\gamma_0, \dots, \gamma_{a-1})$ be the set of all u (necessarily in $U_{M,\min}$ by the previous paragraph) defined by (5.13) with $u^{(k)} \in U^+_{\min}(\gamma_k)$ for $k = 0, \dots, a-1$. We have proved the following result.

Proposition 5.14. *There is a decomposition of $U_{M,\min}$ into disjoint subsets:*

$$U_{M,\min} = \bigcup_{(\gamma_0,\dots,\gamma_{a-1}) \in \Gamma_M} U(\gamma_0, \dots, \gamma_{a-1}).$$

Example 2: Let $A = \{\mathbf{a}_1, \mathbf{a}_2\} \subseteq \mathbb{Z}$, where $\mathbf{a}_1 = 1$ and $\mathbf{a}_2 = -1$. For $\beta \in \mathbb{Z}$ we have $U(\beta) = \{(l+\beta, l) \mid l \in \mathbb{Z}\}$ and $U^+(\beta) = \{(l+\beta, l) \in U(\beta) \mid l \geq \max(0, -\beta)\}$. It is then clear that $w(\beta) = |\beta|$ and that

$$U^+_{\min}(\beta) = \begin{cases} \{(\beta, 0)\} & \text{if } \beta \geq 0, \\ \{(0, -\beta)\} & \text{if } \beta < 0. \end{cases}$$

In particular, β is good if and only if $-(p-1) \leq \beta \leq (p-1)$ and no β is very good. Suppose that $q = p$ and $M = \mathbf{e} + (p-1)\mathbb{Z}$ where $\mathbf{e} \in \mathbb{Z}$. In this case it is easy to compute the decomposition of Proposition 5.14. We may assume $0 \leq \mathbf{e} < p-1$. Then

$$U_{M,\min} = \begin{cases} U^+_{\min}(\mathbf{e}) & \text{if } \mathbf{e} < (p-1)/2, \\ U^+_{\min}(\mathbf{e} - (p-1)) & \text{if } \mathbf{e} > (p-1)/2, \\ U^+_{\min}((p-1)/2) \cup U^+_{\min}(-(p-1)/2) & \text{if } \mathbf{e} = (p-1)/2. \end{cases}$$

Computing the decomposition of Proposition 5.14 is more involved when one is not working over the prime field. We continue with this example when $q = p^2$

and $M = \mathbf{e} + (p^2-1)\mathbb{Z}$ for $\mathbf{e} \in \mathbb{Z}$. We may assume that $\mathbf{e} = e_0 + e_1 p$, where $0 \le e_0, e_1 \le p-1$. Suppose first that $\mathbf{e} = 0$. Then

$$U_M = \{(u,u) \mid 0 \le u \le p^2-1\} \cup \{(p^2-1, 0)\} \cup \{(0, p^2-1)\}.$$

It follows that $U_{M,\min} = \{(0,0)\}$ and $w_p(M) = 0$.

Suppose that $\mathbf{e} \neq 0$. If $(\gamma_0, \gamma_1) \in \Gamma_M$, then in particular both γ_0 and γ_1 are good, so by the above we have

$$-(p-1) \le \gamma_0, \gamma_1 \le (p-1). \tag{5.15}$$

By (5.11) we have $\gamma_0 + p\gamma_1 \in \mathbf{e} + (p^2-1)\mathbb{Z}$, so (5.15) implies that

$$\gamma_0 + p\gamma_1 = \mathbf{e} \tag{5.16}$$

or

$$\gamma_0 + p\gamma_1 = \mathbf{e} - (p^2-1). \tag{5.17}$$

Equation (5.16) has a solution $(\gamma_0, \gamma_1) = (e_0, e_1)$ satisfying (5.15). If $e_0 \neq 0$ and $e_1 \neq p-1$, then $(\gamma_0, \gamma_1) = (e_0 - p, e_1 + 1)$ is also a solution satisfying (5.15). There are no other solutions of (5.16) satisfying (5.15). Equation (5.17) has a solution $(\gamma_0, \gamma_1) = (e_0 - (p-1), e_1 - (p-1))$ satisfying (5.15). If $e_0 \neq p-1$ and $e_1 \neq 0$, then $(\gamma_0, \gamma_1) = (e_0 + 1, e_1 - p)$ is also a solution satisfying (5.15). There are no other solutions of (5.17) satisfying (5.15). For notational convenience we set

$$\Gamma_1 = (e_0, e_1),\ \Gamma_2 = (e_0 - p, e_1 + 1),\ \Gamma_3 = (e_0 - (p-1), e_1 - (p-1)),\ \Gamma_4 = (e_0 + 1, e_1 - p).$$

Since $w(\gamma_i) = |\gamma_i|$, we have $(\gamma_0, \gamma_1) \in \Gamma_M$ if and only if $w_p(M) = |\gamma_0| + |\gamma_1|$. From the definition of $w_p(M)$, we have $\Gamma_1 \in \Gamma_M$ if and only if

$$e_0 + e_1 \le \min\{p - e_0 + e_1 + 1, 2(p-1) - e_0 - e_1, e_0 + 1 + p - e_1\}.$$

Simplifying these inequalities gives

$$\Gamma_1 \in \Gamma_M \text{ if and only if } e_0, e_1 \le (p+1)/2 \text{ and } e_0 + e_1 \le p-1. \tag{5.18}$$

Similar calculations give

$$\Gamma_2 \in \Gamma_M \text{ if and only if } e_0 \ge (p+1)/2 \text{ and } e_1 \le (p-3)/2, \tag{5.19}$$

$$\Gamma_3 \in \Gamma_M \text{ if and only if } e_0, e_1 \ge (p-3)/2 \text{ and } e_0 + e_1 \ge p-1, \tag{5.20}$$

and

$$\Gamma_4 \in \Gamma_M \text{ if and only if } e_0 \le (p-3)/2 \text{ and } e_1 \ge (p+1)/2. \tag{5.21}$$

One then calculates that there are eleven possibilities for Γ_M:

Case 1: $\Gamma_M = \{\Gamma_1\}$ if $e_0 \le (p-3)/2$ and $e_1 < (p+1)/2$ or if $e_0 = (p-1)/2$ and $e_1 < (p-1)/2$.

Case 2: $\Gamma_M = \{\Gamma_3\}$ if $e_0 \ge (p+1)/2$ and $e_1 > (p-3)/2$ or if $e_0 = (p-1)/2$ and $e_1 > (p-1)/2$.

Case 3: $\Gamma_M = \{\Gamma_2\}$ if $e_0 > (p+1)/2$ and $e_1 < (p-3)/2$.

Case 4: $\Gamma_M = \{\Gamma_4\}$ if $e_0 < (p-3)/2$ and $e_1 > (p+1)/2$.

Case 5: $\Gamma_M = \{\Gamma_1, \Gamma_2\}$ if $e_0 = (p+1)/2$ and $e_1 < (p-3)/2$.

Case 6: $\Gamma_M = \{\Gamma_3, \Gamma_4\}$ if $e_0 = (p-3)/2$ and $e_1 > (p+1)/2)$.

Case 7: $\Gamma_M = \{\Gamma_1, \Gamma_3\}$ if $e_0 = e_1 = (p-1)/2$.

Case 8: $\Gamma_M = \{\Gamma_1, \Gamma_4\}$ if $e_0 < (p-3)/2$ and $e_1 = (p+1)/2$.

Case 9: $\Gamma_M = \{\Gamma_2, \Gamma_3\}$ if $e_0 > (p+1)/2$ and $e_1 = (p-3)/2$.

Case 10: $\Gamma_M = \{\Gamma_1, \Gamma_2, \Gamma_3\}$ if $e_0 = (p+1)/2$ and $e_1 = (p-3)/2$.
Case 11: $\Gamma_M = \{\Gamma_1, \Gamma_3, \Gamma_4\}$ if $e_0 = (p-3)/2$ and $e_1 = (p+1)/2$.

6. Hasse invariants

We make precise the relationship between the additive character Ψ and the uniformizer π of the field $\mathbb{Q}_p(\zeta_{q-1}, \zeta_p)$. Fix π satisfying $\pi^{p-1} = -p$. There is a unique p-th root of unity ζ_p with $\zeta_p \equiv 1 + \pi \pmod{\pi^2}$. One defines an additive character $\psi_\pi : \mathbb{F}_p \to \mathbb{Q}_p(\zeta_p)^\times$ by requiring $\psi_\pi(1) = \zeta_p$. The additive character $\Psi : \mathbb{F}_q \to \mathbb{Q}_p(\zeta_{q-1}, \zeta_p)^\times$ is defined to be $\Psi = \psi_\pi \circ \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}$.

We recall the method of Ax[5]. Define a polynomial

$$P(t) = \sum_{r=0}^{q-1} p_r t^r \in \mathbb{Q}_p(\zeta_{q-1}, \zeta_p)[t]$$

by the conditions

$$P(\omega(x)) = \Psi(x) \in \mathbb{Q}_p(\zeta_{q-1}, \zeta_p)$$

for $x \in \mathbb{F}_q$ (we take $\omega(0) = 0$). One computes that $p_0 = 1$, $p_{q-1} = -q/(q-1)$, and that for $1 \le r \le q-2$ one has $p_r = G_r/(q-1)$, where G_r is the Gauss sum

$$G_r = \sum_{z \in \mathbb{F}_q^\times} \omega(z)^{-r} \Psi(z) \in \mathbb{Q}_p(\zeta_{q-1}, \zeta_p).$$

By Stickelberger's Theorem[17] (or see [14, Theorem 4.5]),

$$p_r \equiv \frac{\pi^{S(r)}}{r_0! r_1! \cdots r_{a-1}!} \pmod{\pi^{S(r)+1}}, \tag{6.1}$$

where $r = r_0 + r_1 p + \cdots + r_{a-1} p^{a-1}$ with $0 \le r_k \le p-1$ for $k = 0, \ldots, a-1$ and $S(r) = r_0 + r_1 + \cdots + r_{a-1}$.

For a vector $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{Z}^n$ we set $\omega(x)^{\mathbf{b}} = \omega(x_1)^{b_1} \cdots \omega(x_n)^{b_n}$. We also adopt the convention that $\omega(0)^b = 0$ for $b \ne 0$ but that $\omega(0)^0 = 1$. Then for the exponential sum (1.1) we have

$$\begin{aligned} S(f_\lambda, \mathbf{e}) &= \sum_{x \in (\mathbb{F}_q^\times)^n} \omega(x)^{-\mathbf{e}} \prod_{j=1}^N \Psi(\lambda_j x^{\mathbf{a}_j}) \\ &= \sum_{x \in (\mathbb{F}_q^\times)^n} \omega(x)^{-\mathbf{e}} \prod_{j=1}^N P(\omega(\lambda_j)\omega(x)^{\mathbf{a}_j}) \\ &= \sum_{x \in (\mathbb{F}_q^\times)^n} \omega(x)^{-\mathbf{e}} \prod_{j=1}^N \biggl(\sum_{r=0}^{q-1} p_r \omega(\lambda_j)^r \omega(x)^{r\mathbf{a}_j} \biggr). \end{aligned}$$

Let U_{q-1}^+ be as in Section 5. Then

$$\begin{aligned} S(f_\lambda, \mathbf{e}) &= \sum_{x \in (\mathbb{F}_q^\times)^n} \omega(x)^{-\mathbf{e}} \sum_{u = (u_1, \ldots, u_N) \in U_{q-1}^+} \biggl(\prod_{j=1}^N p_{u_j} \omega(\lambda_j)^{u_j} \biggr) \omega(x)^{\sum_{j=1}^N u_j \mathbf{a}_j} \\ &= \sum_{u \in U_{q-1}^+} \biggl(\prod_{j=1}^N p_{u_j} \omega(\lambda_j)^{u_j} \biggr) \biggl(\sum_{x \in (\mathbb{F}_q^\times)^n} \omega(x)^{-\mathbf{e} + \sum_{j=1}^N u_j \mathbf{a}_j} \biggr). \end{aligned}$$

One has

$$\sum_{x\in(\mathbb{F}_q^\times)^n}\omega(x)^{-\mathbf{e}+\sum_{j=1}^N u_j\mathbf{a}_j}=\begin{cases}(q-1)^n & \text{if } -\mathbf{e}+\sum_{j=1}^N u_j\mathbf{a}_j\in(q-1)\mathbb{Z}^n,\\ 0 & \text{otherwise.}\end{cases}$$

Set $M=\mathbf{e}+(q-1)\mathbb{Z}^n$, so that $U_M=\{u\in U_{q-1}^+\mid \sum_{j=1}^N u_j\mathbf{a}_j\in\mathbf{e}+(q-1)\mathbb{Z}^n\}$. It follows that

$$S(f_\lambda,\mathbf{e})=(q-1)^n\sum_{u\in U_M}\prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j}. \tag{6.2}$$

Note that it can happen that $U_M=\emptyset$ (for example, if $\mathbf{a}_j\in(q-1)\mathbb{Z}^n$ for all j but $\mathbf{e}\notin(q-1)\mathbb{Z}^n$), in which case $S(f_\lambda,\mathbf{e})=0$ for all λ. From now on we assume that $U_M\neq\emptyset$.

Eq. (6.1) implies that

$$\prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j}\equiv\left(\frac{\omega(\lambda_1)^{u_1}\cdots\omega(\lambda_N)^{u_N}}{\prod_{j=1}^N u_j^{(0)}!\cdots u_j^{(a-1)}!}\right)\pi^{w_p(u)}\pmod{\pi^{w_p(u)+1}}$$

where the $u^{(k)}$ are defined by (5.1), so (6.2) gives

$$\begin{aligned}&S(f_\lambda,\mathbf{e})\equiv\\ &\quad(-1)^n\left(\sum_{u\in U_{M,\min}}\frac{\omega(\lambda_1)^{u_1}\cdots\omega(\lambda_N)^{u_N}}{\prod_{j=1}^N u_j^{(0)}!u_j^{(1)}!\cdots u_j^{(a-1)}!}\right)\pi^{w_p(M)}\pmod{\pi^{w_p(M)+1}}.\end{aligned}\tag{6.3}$$

The coefficient of $\pi^{w_p(M)}$ on the right-hand side of (6.3) is a sum of distinct nonzero monomials in $\omega(\lambda_1),\dots,\omega(\lambda_N)$, hence is a nonzero polynomial of degree $\leq q-1$ in each $\omega(\lambda_i)$.

Let $H(\lambda_1,\dots,\lambda_N)$ be the reduction mod p of the coefficient of $\pi^{w_p(M)}$ in Eq. (6.3):

$$\begin{aligned}&H(\lambda_1,\dots,\lambda_N)=\\ &\qquad(-1)^n\sum_{u\in U_{M,\min}}\frac{\lambda_1^{u_1}\cdots\lambda_N^{u_N}}{\prod_{j=1}^N u_j^{(0)}!u_j^{(1)}!\cdots u_j^{(a-1)}!}\in\mathbb{F}_p[\lambda_1,\dots,\lambda_N].\end{aligned}\tag{6.4}$$

By Proposition 5.14 we have

$$H(\lambda_1,\dots,\lambda_N)=(-1)^n\sum_{(\gamma_0,\dots,\gamma_{a-1})\in\Gamma_M}\;\sum_{u\in U(\gamma_0,\dots,\gamma_{a-1})}\frac{\prod_{j=1}^N\prod_{k=0}^{a-1}\lambda_j^{u_j^{(k)}p^k}}{\prod_{j=1}^N\prod_{k=0}^{a-1}u_j^{(k)}!}. \tag{6.5}$$

The inner sum on the right-hand side may be written

$$\prod_{k=0}^{a-1}\sum_{u^{(k)}\in U^+_{\min}(\gamma_k)}\frac{(\lambda_1^{u_1^{(k)}}\cdots\lambda_N^{u_N^{(k)}})^{p^k}}{u_1^{(k)}!\cdots u_N^{(k)}!}.$$

But this expression is just $\prod_{k=0}^{a-1}F_{\gamma_k}(\lambda^{p^k})$, where the F_γ are defined in (2.4). This completes the proof of the following statement, which is our main result.

Theorem 6.6. *The Hasse invariant of the exponential sum $S(f_\lambda,\mathbf{e})$ is*

$$H(\lambda_1,\dots,\lambda_N)=(-1)^n\sum_{(\gamma_0,\dots,\gamma_{a-1})\in\Gamma_M}F_{\gamma_0}(\lambda)F_{\gamma_1}(\lambda^p)\cdots F_{\gamma_{a-1}}(\lambda^{p^{a-1}}).$$

If $H(\lambda_1,\dots,\lambda_N)\neq 0$, then

$$\operatorname{ord}_p S(f_\lambda,\mathbf{e}) = \frac{w_p(M)}{p-1},$$

and if $H(\lambda_1,\dots,\lambda_N)=0$, then

$$\operatorname{ord}_p S(f_\lambda,\mathbf{e}) > \frac{w_p(M)}{p-1}.$$

Example 2 (cont.): We compute the Hasse invariants of the "twisted" Kloosterman sums over $\mathbb{F}_q$ for $q=p,p^2$:

$$\sum_{x\in\mathbb{F}_q^\times} \omega(x)^{-\mathbf{e}}\Psi(\lambda_1 x+\lambda_2/x), \tag{6.7}$$

which corresponds to choosing $A=\{\mathbf{a}_1,\mathbf{a}_2\}\subseteq\mathbb{Z}$, $\mathbf{a}_1=1$, $\mathbf{a}_2=-1$. First take $q=p$, so that $0\le\mathbf{e}<p-1$ and $M=\mathbf{e}+(p-1)\mathbb{Z}$. From Example 2 of the previous section we have immediately

$$H(\lambda)=\begin{cases} -\dfrac{\lambda_1^{\mathbf{e}}}{\mathbf{e}!} & \text{if } \mathbf{e}<(p-1)/2,\\ -\dfrac{\lambda_2^{p-1-\mathbf{e}}}{(p-1-\mathbf{e})!} & \text{if } \mathbf{e}>(p-1)/2,\\ -\dfrac{\lambda_1^{(p-1)/2}+\lambda_2^{(p-1)/2}}{((p-1)/2)!} & \text{if } \mathbf{e}=(p-1)/2.\end{cases}$$

Now consider the case $q=p^2$. We have $0\le\mathbf{e}<p^2-1$ and $M=\mathbf{e}+(p^2-1)\mathbb{Z}$, so we may write $\mathbf{e}=e_0+e_1p$ with $0\le e_0,e_1\le p-1$. In this situation, we computed in Example 2 of the previous section all possibilities for Γ_M with their corresponding elements (γ_0,γ_1). Applying Theorem 6.6 gives the following results, where the case numbers refer to the case specified in Example 2 of Section 5.

Case 1: $H(\lambda)=-\dfrac{\lambda_1^e}{e_0!e_1!}$.

Case 2: $H(\lambda)=-\dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!}$.

Case 3: $H(\lambda)=-\dfrac{\lambda_2^{p-e_0}\lambda_1^{(e_1+1)p}}{(p-e_0)!(e_1+1)!}$.

Case 4: $H(\lambda)=-\dfrac{\lambda_1^{e_0+1}\lambda_2^{(p-e_1)p}}{(e_0+1)!(p-e_1)!}$.

Case 5: $H(\lambda)=-\dfrac{\lambda_1^e}{e_0!e_1!}-\dfrac{\lambda_2^{p-e_0}\lambda_1^{(e_1+1)p}}{(p-e_0)!(e_1+1)!}$.

Case 6: $H(\lambda)=-\dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!}-\dfrac{\lambda_1^{e_0+1}\lambda_2^{(p-e_1)p}}{(e_0+1)!(p-e_1)!}$.

Case 7: $H(\lambda)=-\dfrac{\lambda_1^e}{e_0!e_1!}-\dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!}$.

Case 8: $H(\lambda)=-\dfrac{\lambda_1^e}{e_0!e_1!}-\dfrac{\lambda_1^{e_0+1}\lambda_2^{(p-e_1)p}}{(e_0+1)!(p-e_1)!}$.

Case 9: $H(\lambda)=-\dfrac{\lambda_2^{p-e_0}\lambda_1^{(e_1+1)p}}{(p-e_0)!(e_1+1)!}-\dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!}$.

Case 10: $H(\lambda) = -\dfrac{\lambda_1^e}{e_0!e_1!} - \dfrac{\lambda_2^{p-e_0}\lambda_1^{(e_1+1)p}}{(p-e_0)!(e_1+1)!} - \dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!}$.

Case 11: $H(\lambda) = -\dfrac{\lambda_1^e}{e_0!e_1!} - \dfrac{\lambda_2^{p^2-1-e}}{(p-1-e_0)!(p-1-e_1)!} - \dfrac{\lambda_1^{e_0+1}\lambda_2^{(p-e_1)p}}{(e_0+1)!(p-e_1)!}$.

Remark: In [4] we calculated $w_p(M)$ for the exponential sum (6.7) for all odd q and all $\mathbf{e}$. From the results in that paper, one can also compute the Hasse invariants for those exponential sums.

7. Affine sums

In this section we extend Theorem 6.6 to the case of exponential sums containing some affine variables. Let now

$$f_\lambda = \sum_{j=1}^N \lambda_j x^{\mathbf{a}_j} \in \mathbb{F}_q[x_1^{\pm 1}, \dots, x_m^{\pm 1}, x_{m+1}, \dots, x_n],$$

i.e., the first m variables are toric and the last $n-m$ variables are affine. We are considering the sum

$$S_{\mathrm{aff}}(f_\lambda, \mathbf{e}) = \sum_{x \in (\mathbb{F}_q^\times)^m \times \mathbb{F}_q^{n-m}} \prod_{i=1}^m \omega(x_i)^{-e_i} \Psi(f_\lambda(x)) \in \mathbb{Q}_p(\zeta_p, \zeta_{q-1}), \tag{7.1}$$

where $\mathbf{e} = (e_1, \dots, e_m, 0, \dots, 0) \in \mathbb{Z}^n$. For each subset $I \subseteq \{m+1, \dots, n\}$, let $f_{\lambda,I} \in \mathbb{F}_q[x_1^{\pm 1}, \dots, x_m^{\pm 1}, \{x_i\}_{i \in I}]$ be the Laurent polynomial obtained from f_λ by setting $x_j = 0$ for $j \notin I$, $m+1 \le j \le n$, and let $\mathbf{e}_I = (e_1, \dots, e_m, 0, \dots, 0) \in \mathbb{Z}^{m+|I|}$. As in (1.1), we set

$$S(f_{\lambda,I}, \mathbf{e}_I) = \sum_{x \in (\mathbb{F}_q^\times)^{m+|I|}} \prod_{i=1}^m \omega(x_i)^{-e_i} \Psi(f_{\lambda,I}(x)).$$

Then we have the relation

$$S_{\mathrm{aff}}(f_\lambda, \mathbf{e}) = \sum_{I \subseteq \{m+1, \dots, n\}} S(f_{\lambda,I}, \mathbf{e}_I). \tag{7.2}$$

We identify $\mathbb{Z}^{m+|I|}$ with the subgroup of $\mathbb{Z}^n$ of vectors with j-th coordinate 0 for $j \notin I$. Let $M_I = \mathbf{e}_I + (q-1)\mathbb{Z}^{m+|I|}$ and let A_I be the subset of A consisting of all $\mathbf{a}_i$ with j-th coordinate 0 for $j \notin I$. Then we have

$$U_{M_I} = \{u \in U_M \mid u_i = 0 \text{ for every index } i \text{ for which } \mathbf{a}_i \notin A_I\}.$$

From (6.2) we have

$$S(f_{\lambda,I}, \mathbf{e}_I) = (q-1)^{m+|I|} \sum_{u \in U_{M_I}} \prod_{j=1}^N p_{u_j} \omega(\lambda_j)^{u_j}. \tag{7.3}$$

Combining (7.2) and (7.3) gives

$$S_{\mathrm{aff}}(f_\lambda, \mathbf{e}) = \sum_{I \subseteq \{m+1, \dots, n\}} (q-1)^{m+|I|} \sum_{u \in U_{M_I}} \prod_{j=1}^N p_{u_j} \omega(\lambda_j)^{u_j}. \tag{7.4}$$

The sets U_{M_I} are not disjoint so we gather the contributions on the right-hand side of (7.4) as follows. Fix $u \in U_M$ and let $I_u \subseteq \{m+1, \dots, n\}$ be the set of

indices j such that the j-th coordinate of $\sum_{i=1}^N u_i\mathbf{a}_i$ is nonzero. Then we have $u\in M_I$ if and only if $I_u\subseteq I$, and the contribution of u to the sum (7.4) is

$$\prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j}\sum_{I\supseteq I_u}(q-1)^{m+|I|}=(q-1)^{m+|I_u|}q^{n-m-|I_u|}\prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j}.$$

For $l=0,1,\dots,n-m$, let $M_l\subseteq M$ be the subset of lattice points with j-th coordinate nonzero for exactly l values of $j\in\{m+1,\dots,n\}$. Then $u\in U_{M_l}$ if and only if $|I_u|=l$, so

$$S_{\rm aff}(f_\lambda,\mathbf{e})=\sum_{l=0}^{n-m}(q-1)^{m+l}q^{n-m-l}\sum_{u\in U_{M_l}}\prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j}. \tag{7.5}$$

Note that the sets M_l satisfy condition (5.5), since for $\mathbf{a}=\sum_{i=1}^N c_i\mathbf{a}_i\in\mathbb{N}A\cap M$ the value of l for which $\mathbf{a}\in M_l$ is determined by the set $\{i\in\{1,\dots,N\}\mid c_i>0\}$, and this set is unchanged if some $c_{i_0}\geq q$ is replaced by $c_{i_0}-(q-1)$.

We now impose the hypothesis that for each $j\in\{m+1,\dots,n\}$ there exists $\mathbf{a}_i\in A$ such that the j-th coordinate of $\mathbf{a}_i$ is nonzero, i.e., the set A is not contained in any coordinate hyperplane $x_j=0$, $m+1\leq j\leq n$.

Lemma 7.6. *Assume the above hypothesis. Then for $l=0,1,\dots,n-m$,*

$$w_p(M_l)+a(n-m-l)(p-1)\geq w_p(M_{n-m}).$$

Proof. The assertion is trivial for $l=n-m$ so suppose that $u\in U_{M_l}$ for some $l<n-m$. Then there exists an index j, $m+1\leq j\leq n$, such that $u_i=0$ for all i such that $\mathbf{a}_i$ has nonzero j-th coordinate. By our hypothesis, there exists i_0 such that the j-th coordinate of $\mathbf{a}_{i_0}$ is nonzero. Define

$$u_i'=\begin{cases}u_i & \text{if } i\neq i_0,\\ q-1 & \text{if } i=i_0.\end{cases}$$

Then $I_{u'}\supseteq I_u\cup\{j\}$ so $u'\in U_{M_{l'}}$ for some $l'\geq l+1$. Since $u_{i_0}=0$, it follows that

$$w_p(u')=w_p(u)+a(p-1).$$

If $l'<n-m$ this argument may be repeated until after, say, r steps (with $r\leq n-m-l$) we arrive at $u^{(r)}\in U_{M_{n-m}}$, hence

$$w_p(u^{(r)})=w_p(u)+ar(p-1)\leq w_p(u)+a(n-m-l)(p-1).$$

This inequality implies the lemma. $\square$

Equation (6.1) implies that

$$\mathrm{ord}_p\prod_{j=1}^N p_{u_j}\omega(\lambda_i)^{u_j}=\frac{w_p(u)}{p-1},$$

so

$$\mathrm{ord}_p\, q^{n-m-l}\prod_{j=1}^N p_{u_j}\omega(\lambda_i)^{u_j}=\frac{w_p(u)+(n-m-l)a(p-1)}{p-1}. \tag{7.7}$$

Then Equations (7.5), (7.7), and Lemma 7.6 imply that

$$(7.8)\qquad S_{\mathrm{aff}}(f_\lambda,\mathbf{e}) \equiv {\sum_l}' (-1)^{m+l} \sum_{u\in U_{M_l,\min}} \prod_{j=1}^N p_{u_j}\omega(\lambda_j)^{u_j} \pmod{\pi^{w_p(M_{n-m})+1}},$$

where $\sum_l'$ denotes a sum over those l for which equality holds in Lemma 7.6.

We now apply Proposition 5.14 to decompose $U_{M_l,\min}$: Let Γ_{M_l} be the set of all sequences $(\gamma_0,\dots,\gamma_{a-1})$ of good elements of $\mathbb{Z}^n$ satisfying (5.11) and (5.12) (with M replaced M_l). Then

$$U_{M_l,\min} = \bigcup_{(\gamma_0,\dots,\gamma_{a-1})\in\Gamma_{M_l}} U(\gamma_0,\dots,\gamma_{a-1}).$$

Arguing as in the proof of Theorem 6.6 gives the following result.

Theorem 7.9. *The Hasse invariant of the exponential sum $S_{\mathrm{aff}}(f_\lambda,\mathbf{e})$ is*

$$H(\lambda_1,\dots,\lambda_N) = {\sum_l}'(-1)^{m+l} \sum_{(\gamma_0,\dots,\gamma_{a-1})\in\Gamma_{M_l}} F_{\gamma_0}(\lambda)F_{\gamma_1}(\lambda^p)\cdots F_{\gamma_{a-1}}(\lambda^{p^{a-1}}),$$

where $\sum_l'$ denotes a sum over those l for which equality holds in Lemma 7.6. If $H(\lambda_1,\dots,\lambda_N)\neq 0$, then

$$\operatorname{ord}_p S_{\mathrm{aff}}(f_\lambda,\mathbf{e}) = \frac{w_p(M_{n-m})}{p-1},$$

and if $H(\lambda_1,\dots,\lambda_N)=0$, then

$$\operatorname{ord}_p S_{\mathrm{aff}}(f_\lambda,\mathbf{e}) > \frac{w_p(M_{n-m})}{p-1}.$$

Example 3: Suppose that $\mathbf{a}_j\in\mathbb{N}^n$ with $\sum_{i=1}^n a_{ji} = d > 0$ for all j, i.e., f_λ is a homogeneous polynomial of degree d. We work over $\mathbb{F}_p$ and consider the sum

$$S_{\mathrm{aff}}(x_{n+1}f_\lambda) = \sum_{(x_1,\dots,x_{n+1})\in\mathbb{F}_p^{n+1}} \Psi(x_{n+1}f_\lambda(x_1,\dots,x_n)).$$

If $N_{\mathrm{aff}}(\lambda)$ denotes the number of $\mathbb{F}_p$-rational points on the hypersurface $f_\lambda = 0$ in $\mathbb{A}^n$, then $S_{\mathrm{aff}}(x_{n+1}f_\lambda) = pN_{\mathrm{aff}}(\lambda)$. We assume there exist u_i, $0\le u_i\le p-1$, such that $\sum_{i=1}^N u_i(\mathbf{a}_i,1)\in(p-1)(\mathbb{Z}_{>0})^{n+1}$ and $\sum_{i=1}^N u_i = p-1$. This implies that $w_p(M_{n+1}) = p-1$ (so that $N_{\mathrm{aff}}(\lambda)$ is prime to p for generic λ) and that equality holds in Lemma 7.6 only for $l=n+1$. Theorem 7.9 then gives

$$H(\lambda_1,\dots,\lambda_N) = (-1)^n \sum_{\gamma_0\in\Gamma_{M_{n+1}}} F_{\gamma_0}(\lambda_1,\dots,\lambda_N)$$

and $H(\lambda)\equiv N_{\mathrm{aff}}(\lambda) \pmod p$. Let $\Gamma_{M_{n+1}} = \{\gamma_0^{(1)},\dots,\gamma_0^{(r)}\}$. Then

$$F_{\gamma_0^{(j)}}(\lambda_1,\dots,\lambda_N) = \sum_{\sum_i u_i(\mathbf{a}_i,1)=\gamma_0^{(j)}} \frac{\lambda_1^{u_1}\cdots\lambda_N^{u_N}}{u_1!\cdots u_N!},$$

where the sum is over all N-tuples $(u_1,\dots,u_N)$, $0\le u_i\le p-1$ for all i, such that $\sum_{i=1}^N u_i(\mathbf{a}_i,1) = \gamma_0^{(j)}\in(p-1)(\mathbb{Z}_{>0})^{n+1}$ and $\sum_{i=1}^N u_i = p-1$. Note that $(p-1)!F_{\gamma_0^{(j)}}(\lambda)$ is the coefficient of $x^{\gamma_0^{(j)}}$ in $(x_{n+1}f_\lambda(x))^{p-1}$. It now follows from Katz[13, Algorithm 2.3.7.14] that $(-1)^{n+1}H(\lambda)$ is congruent mod p to the trace

of the Hasse-Witt matrix associated to the projective hypersurface with equation $f_\lambda = 0$.

References

[1] Adolphson, Alan and Sperber, Steven. Twisted Kloosterman sums and p-adic Bessel functions, II: Newton polygons and analytic continuation. Amer. J. Math. **109** (1987), 723–764.
[2] Adolphson, Alan and Sperber, Steven. p-adic estimates for exponential sums. p-adic analysis (Trento, 1989), 11–22, Lecture Notes in Math., 1454, Springer, Berlin, 1990.
[3] Adolphson, Alan and Sperber, Steven. Exponential sums nondegenerate relative to a lattice. Algebra and Number Theory **3** (2009), 881–906.
[4] Adolphson, Alan and Sperber, Steven. On unit root formulas for toric exponential sums. Algebra and Number Theory **6** (2012), 573–585.
[5] Ax, James. Zeroes of polynomials over finite fields. Amer. J. Math. **86** (1964), 255–261.
[6] Beukers, Frits. Algebraic A-hypergeometric functions. Invent. Math. **180** (2010), no. 3, 589–610.
[7] Blache, Régis. p-density and applications. J. Number Theory (to appear), arXiv:0812.3382.
[8] Blache, Régis. First vertices for generic Newton polygons. arXiv:0912.2051.
[9] Blache, Régis. Congruences for L-functions of additive exponential sums. arXiv: 1206.1387.
[10] Dwork, Bernard. p-adic cycles. Inst. Hautes Études Sci. Publ. Math. **37** (1969), 27–115.
[11] Dwork, Bernard. Bessel functions as p-adic functions of the argument. Duke Math. J. **41** (1974), 711–738.
[12] Igusa, Jun-ichi. Class number of a definite quaternion with prime discriminant. Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.
[13] Katz, Nicholas. Algebraic solutions of differential equations (p-curvature and the Hodge filtration). Invent. Math. **18** (1972), 1–118.
[14] Lang, Serge. Cyclotomic fields. II. Graduate Texts in Mathematics, 69. Springer-Verlag, New York-Berlin, 1980.
[15] Moreno, Oscar; Shum, Kenneth W.; Castro, Francis N.; Kumar, P. Vijay. Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications. Proc. London Math. Soc. (3) **88** (2004), no. 3, 545–564.
[16] Saito, Mutsumi; Sturmfels, Bernd; Takayama, Nobuki. Gröbner deformations of hypergeometric differential equations. Algorithms and Computation in Mathematics, 6. Springer-Verlag, Berlin, 2000.
[17] Stickelberger, Ludwig. Ueber eine Verallgemeinerung der Kreistheilung. Math. Ann. **37** (1890), no. 3, 321–367.

Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma 74078
E-mail address: `adolphs@math.okstate.edu`

School of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455
E-mail address: `sperber@math.umn.edu`